

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S): KIM, Hoe-Won
SERIAL NO.: Not Yet Assigned
FILED: Herewith
FOR: **SECURITY DECIPHERING APPARATUS FOR
ENCIPHERED DATA TRANSMITTED OVER PUBLIC
NETWORK AND SECURITY DECIPHERING METHOD
USING THE SAME**
DATED: January 9, 2004

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF PRIORITY DOCUMENTS

Sir:

Enclosed is a certified copy of Korean Patent Appln. No. 1734-
2003 filed on January 9, 2003, from which priority is claimed under 35 U.S.C.
§119.

Respectfully submitted,



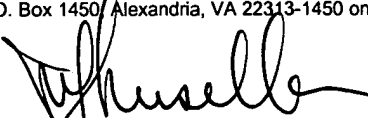
Paul J. Farrell, Esq.
Reg. No. 33,494
Attorney for Applicant(s)

DILWORTH & BARRESE, LLP
333 Earle Ovington Blvd.
Uniondale, NY 11553
(516) 228-8484

CERTIFICATION UNDER 37 C.F.R. 1.10

I hereby certify that this New Application Transmittal and the documents referred to as enclosed therein are being deposited with the United States Postal Service in an envelope as "Express Mail Post Office to Addressee" Mail Label Number EL 995744686 US addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date listed below.

Dated: January 9, 2004



Michael J. Musella



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Intellectual
Property Office.

출 원 번 호 : 10-2003-0001734
Application Number

출 원 년 월 일 : 2003년 01월 10일
Date of Application JAN 10, 2003

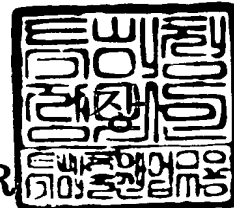
출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.



2003 년 03 월 06 일

특 허 청

COMMISSIONER



【서지사항】

【서류명】	특허출원서		
【권리구분】	특허		
【수신처】	특허청장		
【참조번호】	0006		
【제출일자】	2003.01.10		
【국제특허분류】	H04B		
【국제특허분류】	H04K		
【발명의 명칭】	공공 네트워크를 통해 전송된 데이터를 판독하기 위한 보안 판독장치 및 이를 이용한 데이터의 보안 판독 방법		
【발명의 영문명칭】	SECURITY DECIPHER APPARATUS FOR DECIPHERING DATA TRANSMITTED OVER PUBLIC NETWORK AND METHOD FOR DECIPHERING SECURITY OF THE DATA USING THAT		
【출원인】			
【명칭】	삼성전자 주식회사		
【출원인코드】	1-1998-104271-3		
【대리인】			
【성명】	이건주		
【대리인코드】	9-1998-000339-8		
【포괄위임등록번호】	2003-001449-1		
【발명자】			
【성명의 국문표기】	김회원		
【성명의 영문표기】	KIM, Hoe Won		
【주민등록번호】	731109-1530614		
【우편번호】	156-826		
【주소】	서울특별시 동작구 사당1동 1034-39 202호		
【국적】	KR		
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 다 리인 주 (인) 이권		
【수수료】			
【기본출원료】	20	면	29,000 원
【가산출원료】	7	면	7,000 원



1020030001734

출력 일자: 2003/3/7

【우선권주장료】	0	건	0	원
【심사청구료】	0	항	0	원
【합계】	36,000			원

【요약서】**【요약】**

보안 판독 장치가 개시된다. 보안 판독장치는, 할당된 고유아이디정보인 고유비밀키(Kh)를 저장하는 고유비밀키 저장부, 공공 네트워크를 통해 수신된 고유비밀키(Kh)에 의해 암호키(Ks)가 암호화된 모듈비밀키($\{Ks\}Kh$)로부터 암호키(Ks)를 디코딩하는 제1디코딩부, 및 암호키(Ks)를 이용하여 공공 네트워크를 통해 수신된 데이터(M)가 암호화된 암호데이터($\{M\}Ks$)로부터 데이터(M)를 디코딩하는 제2디코딩부를 갖는다. 이에 따라, 보안성이 유지된 데이터(M)를 수신할 수 있다.

【대표도】

도 1

【색인어】

데이터 보안, 공공 네트워크, 고유비밀키, 모듈비밀키, 암호, 통신단말기

【명세서】

【발명의 명칭】

공공 네트워크를 통해 전송된 데이터를 판독하기 위한 보안 판독장치 및 이를 이용한 데이터의 보안 판독 방법{SECURITY DECIPHER APPARATUS FOR DECIPHERING DATA TRANSMITTED OVER PUBLIC NETWORK AND METHOD FOR DECIPHERING SECURITY OF THE DATA USING THAT}

【도면의 간단한 설명】

도 1은 본 발명에 따른 데이터 서비스 공급장치의 바람직한 실시 예를 도시한 블록도,

도 2는 본 발명에 따른 데이터 서비스 공급장치를 이용한 데이터 서비스 공급방법의 바람직한 실시 예를 도시한 순서도,

도 3은 도 1의 통신단말기를 보다 상세히 도시한 블록도,

도 4는 도 3의 보안판독모듈을 보다 상세히 도시한 블록도, 그리고

도 5는 본 발명에 따른 보안 판독 장치를 이용한 데이터의 암호 판독 방법의 바람직한 실시 예를 도시한 순서도이다.

* 도면의 주요 부분에 대한 부호의 설명 *

100 : 데이터 서비스 공급장치 110 : 제어부

120 : 데이터(M)데이터베이스 130 : 고유비밀키(Kh)데이터베이스

140 : 송수신부 150 : 데이터(M)암호화부

160 : 고유비밀키(Kh)암호화부 400 : 보안판독모듈
 410 : 모듈비밀키(Kp)저장부 430 : 고유비밀키(Kh)저장부
 450 : 제1디코딩부 470 : 암호키(Ks)저장부
 490 : 제2디코딩부

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<14> 본 발명은 보안 판독장치 및 방법에 관한 것으로서, 보다 상세하게는, 단말의 고유 아이디정보에 의한 디코딩을 통해 실제 암호키를 획득할 수 있도록 함으로써 공공 네트워크를 통해 전송된 데이터에 대해서도 향상된 보안성을 가지고 데이터를 판독할 수 있는 보안 판독장치 및 방법에 관한 것이다.

<15> 현재에 다양한 무선망, 초고속 통신망 등등을 위시한 공공 네트워크의 확충은 온라인(online) 상에서 대량의 데이터 공유를 가능케 하고 있다. 또한, CD 및 DVD 등과 같은 저렴한 대용량 저장매체를 통한 오프라인(offline) 상에서의 데이터 공유도 매우 폭넓게 이용되고 있는 실정이다. 따라서, 사용자는 온라인 및 오프라인을 통해 공유된 수많은 종류의 데이터를 제공받을 수 있다.

<16> 이러한 온라인 및 오프라인 공유 체계는 다양하면서도 대량의 데이터를 사용자에게 용이하게 제공하고 있는데 반하여, 상업성을 띠는 여러 종류의 멀티미디어데이터 또는 보안이 필요한 데이터들에 대한 보안 체계는 매우 취약한 구조를 갖는다.

- <17> 이러한 온라인 및 오프라인을 통한 공유 데이터에 대한 보안의 취약성을 해결하기 위해, 서비스 제공자들은 소정의 보안 채널을 이용하여 허가된 사용자의 단말기에만 해당 데이터를 제공하는 방식을 취하고 있다. 이러한 보안 채널을 통한 데이터의 서비스 방식 중 대표적인 예로는 아래 상술되는 두 가지를 들 수 있다.
- <18> 첫째, 서비스 제공자가 온라인 상에서 사용자의 단말기와의 인증과정을 거친 후, 전용 보안 채널을 통해 데이터를 제공하는 방식이다. 이러한 방식은 상기에서 예시한 다양한 온라인 및 오프라인의 네트워크를 사용하지 못하고, 서비스 제공자로부터 제공되는 전용 보안 채널을 통해서만 서비스를 제공하는 문제점이 있다. 이는 해당 서비스를 제공받기 위해서 미리 인증과정을 거친 후 전용 보안 채널을 통해 서비스를 제공받아야 하기 때문에, 서비스를 제공받기 위한 사용자에게 불편함 및 서비스 이용에 따라 과금되는 비용의 부담을 초래하게 된다.
- <19> 둘째, 특정 사용자의 단말기만이 판독 가능하도록 암호화된 데이터를 일반 네트워크 상에 제공하는 방식이다. 이러한 방식은 사용자가 다양한 방법을 통해 암호화된 데이터를 제공받을 수 있다. 그러나, 이러한 방식으로 데이터 서비스를 제공하는 서비스 공급자는 사용자 단말기 각각에 대응하여 판독 가능한 별도의 암호화정보를 각각의 단말기에 제공해야 하는 문제점이 있다. 이에 따라, 서비스 공급자는 등록된 단말기 별로 서로 다른 암호화정보를 저장하기 위한 저장장치가 필요하게 된다. 또한, 서비스 공급자는 일반 네트워크 상에서 사용자에게 데이터 서비스를 제공하기 위해 필요한 통신장치를 구비해야 함으로 인한 고비용성 및 비효율성을 초래하게 된다.

【발명이 이루고자 하는 기술적 과제】

<20> 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 상업성 데이터 및 보안성 데이터에 대한 보안성을 유지하면서, 일반 공공의 온라인 및 오프라 네트워크를 통해 사용자에게 상업성 데이터 및 보안성 데이터를 제공할 수 있는 데이터 서비스 공급장치 및 이로부터 제공된 데이터를 판독할 수 있는 보안 판독 장치 및 이를 이용한 데이터 제공 방법을 제공하는데 있다.

<21> 본 발명이 다른 목적은, 데이터가 암호화될 때 이용된 암호키를 디코딩을 통해 획득할 수 있도록 함으로서 암호화되어 전송된 데이터를 데이터의 전송을 요구한 디바이스에서만 판독이 가능하도록 데이터에 대한 보안성을 가지고 제공받을 수 있는 보안 판독 장치 및 이를 이용한 보안 판독 방법을 제공하는데 있다.

【발명의 구성 및 작용】

<22> 상기와 같은 목적은 본 발명에 따라, 할당된 고유아이디정보인 고유비밀키(Kh)를 저장하는 고유비밀키 저장부, 공공 네트워크를 통해 수신된 고유비밀키(Kh)에 의해 암호키(Ks)가 암호화된 모듈비밀키({Ks}Kh)로부터 암호키(Ks)를 디코딩하는 제1디코딩부, 및 암호키(Ks)를 이용하여 공공 네트워크를 통해 수신된 데이터(M)가 암호화된 암호데이터({M}Ks)로부터 데이터(M)를 디코딩하는 제2디코딩부를 포함하는 보안 판독 장치에 의해 달성된다.

<23> 바람직하게는, 보안 판독 장치는 모듈비밀키 저장부 및 암호키 저장부를 더 갖는다. 이때, 모듈비밀키 저장부는 공공 네트워크를 통해 전송된 모듈비밀키({Ks}Kh)를 저장하

고, 제1디코딩부의 제어에 따라 저장된 모듈비밀키($\{K_s\}K_h$)를 제1디코딩부로 출력한다.
 암호키 저장부는 제1디코딩부에서 디코딩된 암호키(K_s)를 저장하고, 제2디코딩부의 제어에 따라 저장된 암호키(K_s)를 제2디코딩부로 출력한다.

<24> 한편, 상기와 같은 목적은 본 발명에 따라, 통신단말기에서 요구한 데이터를 서비스하는 데이터 서비스 공급장치에 있어서, 통신단말기에 제공하기 위한 데이터(M)를 저장하는 데이터 데이터베이스, 통신단말기에 마련되어 데이터를 판독하는 보안판독모듈의 고유아이디정보에 대응하는 고유비밀키(K_h)를 저장하는 고유비밀키 데이터베이스, 통신단말기와 공공네트웍을 통해 상호 통신을 수행하는 송수신부, 데이터(M)를 해당 암호키(K_s)를 이용하여 암호화하는 데이터 암호화부, 암호키(K_s)를 고유비밀키(K_h)를 이용하여 암호화하는 고유비밀키 암호화부, 및 데이터 암호화부 및 고유비밀키 암호화부의 암호화 동작을 제어하고 암호화된 암호데이터($\{M\}K_s$) 및 모듈비밀키($\{K_s\}K_h$)를 공공네트웍을 통해 통신단말기에 제공하도록 송수신부를 제어하는 제어부를 포함하는 데이터 서비스 공급장치에 의해 달성된다.

<25> 바람직하게는, 보안판독모듈은, 보안판독모듈에 할당된 고유아이디정보인 고유비밀키(K_h)를 저장하는 고유비밀키 저장부, 고유비밀키(K_h)를 이용하여 송수신부에서 제공된 모듈비밀키($\{K_s\}K_h$)로부터 암호키(K_s)를 디코딩하는 제1디코딩부, 및 암호키(K_s)를 이용하여 송수신부에서 제공된 암호데이터($\{M\}K_s$)로부터 데이터(M)를 디코딩하는 제2디코딩부를 갖는다.

<26> 또한, 상기 보안판독모듈은, 송수신부에서 제공된 모듈비밀키($\{K_s\}K_h$)를 저장하고 제1디코딩부의 제어에 따라 저장된 모듈비밀키($\{K_s\}K_h$)를 제1디코딩부로 출력하는 모듈

비밀키 저장부, 및 제1디코딩부에서 디코딩된 암호키(K_s)를 저장하고 제2디코딩부의 제어에 따라 저장된 암호키(K_s)를 제2디코딩부로 출력하는 암호키 저장부를 더 갖는다.

<27> 한편, 상기와 같은 목적은 본 발명에 따라, a) 할당된 고유아이디정보인 고유비밀키(K_h)에 대해 암호화된 모듈비밀키($\{K_s\}K_h$)의 수신여부를 판단하는 단계, b) 모듈비밀키($\{K_s\}K_h$)가 수신된 것으로 판단되면 고유비밀키(K_h)를 이용하여 모듈비밀키($\{K_s\}K_h$)로부터 암호키(K_s)를 디코딩하는 단계, c) 전송을 요구한 데이터(M)가 암호키(K_s)에 의해 암호화된 암호데이터($\{M\}K_s$)의 수신 여부를 판단하는 단계, 및 d) 암호데이터($\{M\}K_s$)가 수신된 것으로 판단되면 암호키(K_s)를 이용하여 암호데이터($\{M\}K_s$)로부터 데이터(M)를 디코딩하는 단계를 포함하는 보안 판독 장치를 이용한 암호 판독 방법에 의해 달성된다.

<28> 한편, 상기와 같은 목적은 본 발명에 따라, 통신단말기에서 요구한 데이터를 서비스하는 데이터 서비스 공급장치를 이용한 데이터 서비스 공급방법에 있어서, 통신단말기로부터 공공 네트워크를 통해 전송된 데이터(M)의 전송 요구를 수신하는 단계; 수신된 데이터의 전송 요구에 따라 데이터(M)를 해당 암호키(K_s)를 이용하여 암호화하는 단계; 수신된 데이터의 전송 요구에 따라 통신단말기에 마련되어 데이터(M)가 암호화된 암호데이터($\{M\}K_s$)를 디코딩하는 보안판독모듈의 고유아이디정보에 대응하는 고유비밀키(K_h)를 이용하여 암호키(K_s)를 암호화하는 단계; 및 암호화된 암호데이터($\{M\}K_s$) 및 모듈비밀키($\{K_s\}K_h$)를 공공네트워크를 통해 통신단말기에 전송하는 단계를 포함하는 데이터 서비스 공급장치를 이용한 데이터 서비스 공급방법에 의해 달성된다.

<29> 바람직하게는, 상기 통신단말기에 마련된 상기 보안판독모듈은, 보안판독모듈에 할당된 고유아이디정보인 상기 고유비밀키(K_h)를 저장하는 고유비밀키 저장부; 고유비밀키

암호화부에서 암호화된 상기 모듈비밀키($\{K_s\}K_h$)로부터 암호키(K_s)를 디코딩하는 제1디코딩부; 및 암호키(K_s)를 이용하여 데이터 암호화부에서 암호화된 암호데이터($\{M\}K_s$)로부터 데이터(M)를 디코딩하는 제2디코딩부를 갖는다.

<30> 또한, 상기 보안판독모듈은, 송수신부로부터 제공된 모듈비밀키($\{K_s\}K_h$)를 저장하고, 제1디코딩부의 제어에 따라 저장된 모듈비밀키($\{K_s\}K_h$)를 제1디코딩부로 출력하는 모듈비밀키 저장부; 및 제1디코딩부에서 디코딩된 암호키(K_s)를 저장하고, 제2디코딩부의 제어에 따라 저장된 암호키(K_s)를 제2디코딩부로 출력하는 암호키 저장부를 더 갖는다.

<31> 한편, 상기과 같은 목적은 본 발명에 따라, 공공 네트워크를 통해 데이터(M)가 암호키(K_s)에 의해 암호화된 암호데이터($\{M\}K_s$)를 수신하는 이동통신 단말기에 있어서, 할당된 소정의 고유 아이디 정보인 고유비밀키(K_h)를 저장하는 고유비밀키 저장부, 고유비밀키(K_h)로 암호화된 모듈비밀키($\{K_s\}K_h$)를 수신하면 모듈비밀키($\{K_s\}K_h$)로부터 암호키(K_s)를 디코딩하는 제1디코딩부, 및 암호키(K_s)를 이용하여 암호데이터($\{M\}K_s$)로부터 데이터(M)를 디코딩하는 제2디코딩부를 포함하는 보안 판독 장치에 의해 달성된다.

<32> 본 발명에 따르면, 고유비밀키(K_h)암호화부를 통해 암호화된 모듈비밀키($\{K_s\}K_h$)를 통신단말기에 고유하게 할당된 고유비밀키(K_h)에 의한 디코딩을 통해서만 데이터(M)를 암호화할 때 이용된 암호키(K_s)를 획득할 수 있도록 함으로써, 공공 네트워크를 통해 암호화된 암호데이터($\{M\}K_s$)를 유통하더라도 데이터에 대한 향상된 보안성을 제공할 수 있다.

<33> 이하, 본 발명의 바람직한 실시 예들을 첨부한 도면을 참조하여 상세히 설명한다. 도면들 중 동일한 구성요소들은 가능한 한 어느 곳에서든지 동일한 부호들로 나타내고

있음에 유의해야 한다. 또한 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다.

<34> 도 1은 본 발명에 따른 데이터 서비스 공급장치의 바람직한 실시 예를 도시한 블록도이다. 도시된 바와 같이, 데이터 서비스 공급장치는, 제어부(110), 데이터(M) 데이터베이스(120), 고유비밀키 데이터베이스(130), 송수신부(140), 데이터(M)암호화부(150), 및 고유비밀키(Kh)암호화부(160)를 갖는다. 이때 데이터 서비스 공급장치(100)는 공공 네트워크(50)을 통해 통신단말기(200)와 상호 통신을 수행한다.

<35> 제어부(110)는 데이터 서비스 공급장치(100)의 전반적인 동작을 제어한다. 데이터(M) 데이터베이스(120)는 통신단말기(200)에 제공하기 위한 데이터(M)를 저장하고, 제어부(110)의 제어에 따라 저장된 데이터(M)를 제어부(110)에 제공한다. 이때 데이터(M)의 유형은 상업성 데이터 및 보안성 데이터 등을 총칭한다. 고유비밀키 데이터베이스(130)는 통신단말기(200)에 마련되어 데이터(M)를 판독하는 보안판독모듈(400)의 고유아이디정보에 대응하는 고유비밀키(hidden secret key : Kh)를 저장하고, 제어부(110)의 제어에 따라 저장된 고유비밀키(Kh)를 제어부(110)에 제공한다.

<36> 송수신부(140)는 제어부(110)의 제어에 따라 공공네트워크(50)을 통해 통신단말기(200)와 상호 통신을 수행한다. 데이터(M)암호화부(150)는 제어부(110)의 제어에 따라 데이터(M)데이터베이스(120)에 저장된 데이터(M)를 설정된 암호키(Ks)를 이용하여 암호화한다. 고유비밀키(Kh)암호화부(160)는 제어부(110)의 제어에 따라 고유비밀키(Kh)데이터베이스(130)에 저장된 고유비밀키(Kh)를 이용하여 데이터를 암호화할 때 이용된 암호키(Ks)를 암호화한다.

- <37> 이에 따라, 송수신부(140)는 데이터(M)암호화부(150)에 의해 암호화된 암호데이터({M}Ks) 및 고유비밀키(Kh)암호화부(160)에 의해 암호화된 모듈비밀키(personal secret key : {Ks}Kh = Kp)를 공공네트워크(50)를 통해 데이터(M)의 제공을 요구한 통신단말기(200)에 전송한다.
- <38> 따라서, 데이터(M)암호화부(150) 및 고유비밀키(Kh)암호화부(160)를 통해 암호화된 암호데이터({M}Ks) 및 모듈비밀키({Ks}Kh)를 공공네트워크(50)를 통해 통신단말기(200)에 전송함으로써, 데이터에 대한 상업성 및 보안성을 제공할 수 있다.
- <39> 도 2는 본 발명에 따른 데이터 서비스 공급장치를 이용한 데이터 서비스 공급방법의 바람직한 실시 예를 도시한 순서도이다.
- <40> 먼저, 제어부(110)는 송수신부(140)를 통해 통신단말기(200)로부터 데이터(M)의 전송 요구신호가 수신되었는지를 판단한다(S100). 데이터(M)의 전송 요구신호가 수신되지 않은 것으로 판단되면, 제어부(110)는 데이터 서비스의 공급 대기 상태를 유지한다(S180).
- <41> 데이터(M)의 전송 요구신호가 수신된 것으로 판단되면, 제어부(110)는 수신된 데이터의 전송 요구에 대응하는 데이터(M)를 데이터(M)데이터베이스(120)로부터 인출하고, 인출된 데이터(M)를 설정된 암호키(Ks)를 이용하여 암호화하도록 데이터(M)암호화부(150)를 제어한다(S120). 제어부(110)는 통신단말기(200)로부터 전송된 데이터의 전송 요구에 따라 고유비밀키(Kh)데이터베이스(130)로부터 보안판독모듈(400)의 고유아이디정보에 대응하는 고유비밀키(Kh)를 인출하여 데이터(M)를 암호화할 때 이용되는 암호키(Ks)를 암호화하도록 고유비밀키(Kh)암호화부(160)를 제어한다(S140).

- <42> 제어부(110)는 암호화된 암호데이터($\{M\}K_s$) 및 모듈비밀키($\{K_s\}K_h$)를 공공네트워크(50)을 통해 통신단말기(200)에 전송하도록 송수신부(140)를 제어한다(S160). 이에 따라, 송수신부(140)는 공공네트워크(50)을 통해 암호데이터($\{M\}K_s$) 및 모듈비밀키($\{K_s\}K_h$)를 통신단말기(200)에 전송한다.
- <43> 따라서, 데이터(M)암호화부(150) 및 고유비밀키(K_h)암호화부(160)를 통해 암호화된 암호데이터($\{M\}K_s$) 및 모듈비밀키($\{K_s\}K_h$)를 공공네트워크(50)을 통해 통신단말기(200)에 전송함으로써, 데이터에 대한 상업성 및 보안성을 제공할 수 있다.
- <44> 도 3은 도 1의 통신단말기(200)를 보다 상세히 도시한 블록도이다. 도시된 바와 같이, 통신단말기(200)는 제어부(210), 키입력부(230), 표시부(250), 메모리(270), 보안판독모듈(400), 송신부(290), 수신부(330), 듀플렉서(310), 음성처리부(350), 및 음성저장부(370)를 갖는다.
- <45> 제어부(210)는 통신단말기(200)의 전반적인 동작을 제어한다. 키입력부(230)는 다수의 다이얼링 디지트 키와, 메뉴키 및 송출키 등을 구비하며, 사용자가 선택한 키에 해당하는 키신호를 발생시하여 제어부(210)로 제공한다. 표시부(250)는 LCD(Liquid Crystal Display Unit) 및 LED 등으로 구현되며, 제어부(210)의 제어에 따라 수행되는 통신단말기(200)의 제어 데이터 및 입력되는 데이터를 디스플레이 한다.
- <46> 메모리(270)는 통신단말기(200)의 제어 프로그램 및 제어부(210)의 제어에 따라 발생하는 제어 데이터를 저장한다. 보안판독모듈(400)은 데이터 서비스 공급장치(100)로부터 전송된 암호데이터($\{M\}K_s$) 및 모듈비밀키($\{K_s\}K_h$)를 판독하여 데이터(M)를 복원한다. 송신부(290)는 제어부(210)에서 발생한 신호를 입력하여 디지털 무선 변조하여 듀플렉서(310)로 전달한다. 듀플렉서(310)는 송신부(290)로부터 전달받은 무선 신호를 안

테나를 통해 송출하며, 안테나를 통해 수신되는 신호를 수신부(330)로 전달한다. 수신부(330)는 듀플렉서(310)로부터 전달받은 무선 신호를 복조하여 제어부(210)로 전달하고, 제어부(210)는 전달받은 신호에 상응하여 통화를 제어한다.

<47> 음성처리부(350)는 제어부(210)의 제어에 따라 음성저장부(370)로부터 독출된 음성 메시지를 아날로그 처리하여 스피커를 통해 송출하며, 또한 마이크를 통해 사용자로부터 입력되는 아날로그 음성을 디지털 신호 처리한다. 음성저장부(370)는 다수의 음성 메시지를 저장한다.

<48> 본 실시 예에 따라, 제어부(210)는 키입력부(230)를 통해 데이터 전송 요구신호가 입력되면, 송신부(290)를 통해 데이터 전송 요구신호를 데이터 서비스 공급장치(100)에 전송한다.

<49> 데이터 서비스 공급장치(100)로부터 데이터 전송 요구신호에 대응하여 전송된 암호 데이터($\{M\}K_s$) 및 모듈비밀키($\{K_s\}K_h$)가 수신되면, 제어부(210)는 보안판독모듈(400)을 통해 암호데이터($\{M\}K_s$) 및 모듈비밀키($\{K_s\}K_h$)를 판독하여 데이터(M)를 복원한다.

<50> 도 4는 도 3의 보안판독모듈(400)을 보다 상세히 도시한 블록도이다. 보안판독모듈(400)은, 모듈비밀키(K_p)저장부(410), 고유비밀키(K_h)저장부(430), 제1디코딩부(450), 암호키(K_s)저장부(470), 및 제2디코딩부(490)를 갖는다.

<51> 모듈비밀키(K_p)저장부(410)는 도 1의 데이터 서비스 공급장치(100)의 송수신부(140)로부터 전송되어 통신단말기(200)의 수신부(330)에 수신된 모듈비밀키($\{K_s\}K_h$)를 저장한다. 모듈비밀키(K_p)저장부(410)는 제1디코딩부(450)의 제어에 따라 저장된 모듈비밀키($\{K_s\}K_h$)를 제1디코딩부(450)로 출력한다. 고유비밀키(K_h)저장부(430)는 보안판

독모듈(400)에 할당된 고유아이디정보인 고유비밀키(Kh)를 저장한다. 제1디코딩부(450)는 아래 [수학식 1]과 같이 고유비밀키(Kh)저장부(430)에 저장된 고유비밀키(Kh)를 이용하여 데이터 서비스 공급장치(100)의 고유비밀키(Kh) 암호화부(160)에서 암호화된 모듈비밀키($\{K_s\}K_h$)로부터 암호키(K_s)를 디코딩한다.

<52> 【수학식 1】 $\{\{K_s\}K_h\}K_h = K_s$

<53> 암호키(K_s)저장부(470)는 제1디코딩부(450)에서 디코딩된 암호키(K_s)를 저장한다. 암호키(K_s)저장부(470)는 제2디코딩부(490)의 제어에 따라 저장된 암호키(K_s)를 제2디코딩부(490)로 출력한다. 제2디코딩부(490)는 아래 [수학식 2]와 같이 암호키(K_s)저장부(470)에서 출력된 암호키(K_s)를 이용하여 데이터 서비스 공급장치(100)의 데이터(M) 암호화부(150)에서 암호화된 암호데이터($\{M\}K_s$)로부터 데이터(M)를 디코딩한다.

<54> 【수학식 2】 $\{M\}K_s\}K_s = M$

<55> 이와 같이 디코딩된 데이터(M)는 도 3의 제어부(210)에 제공되고, 제어부(210)는 디코딩된 데이터(M)를 해당 프로세스에 따라 표시부(250) 및 음성처리부(350)에 출력한다.

<56> 도 5는 본 발명에 따른 보안 판독 장치를 이용한 데이터의 암호 판독 방법의 바람직한 실시 예를 도시한 순서도이다. 먼저, 통신단말기(200)의 제어부(210)는 데이터 서비스 제공장치(100)로부터 전송된 모듈비밀키($K_p=\{K_s\}K_h$)의 수신 여부를 판단한다(S200). 모듈비밀키($\{K_s\}K_h$)가 수신된 것으로 판단되면, 제어부(210)는 수신된 모듈비밀키($\{K_s\}K_h$)를 모듈비밀키(K_p)저장부(410)에 저장한다(S220).

<57> 제1디코딩부(450)는 모듈비밀키(K_p)저장부(410)에 저장된 모듈비밀키($\{K_s\}K_h$)를 고유비밀키(K_h)저장부(430)에 저장된 고유비밀키(K_h)를 이용하여 암호키(K_s)를 디코딩한다(S240). 암호키(K_s)저장부(470)는 제1디코딩부(450)에서 디코딩된 암호키(K_s)를 저장한다(S260).

<58> 제어부(210)는 데이터 서비스 공급장치(100)로부터 전송된 암호데이터($\{M\}K_s$)의 수신 여부를 판단한다(S280). 암호데이터($\{M\}K_s$)가 수신된 것으로 판단되면, 제2디코딩부(490)는 암호키(K_s)저장부(470)에 저장된 암호키(K_s)를 이용하여 암호데이터($\{M\}K_s$)로부터 데이터(M)를 디코딩한다(S320).

<59> 이에 따라, 제어부(210)는 디코딩된 데이터(M)를 데이터유형에 따라 표시부(270) 및/또는 음성처리부(350)에 출력한다.

<60> 따라서, 암호화된 암호데이터($\{M\}K_s$) 및 모듈비밀키($\{K_s\}K_h$)를 제1디코딩부(450) 및 제2디코딩부(490)를 통해 디코딩하여 요구한 데이터(M)를 복원함으로써, 데이터(M)에 대한 보안성이 유지된 데이터(M)를 수신할 수 있다.

【발명의 효과】

<61> 본 발명에 따르면, 고유비밀키(K_h)암호화부를 통해 암호화된 모듈비밀키($\{K_s\}K_h$)를 통신단말기에 고유하게 할당된 고유비밀키(K_h)에 의한 디코딩을 통해서만 데이터(M)를 암호화할 때 이용된 암호키(K_s)를 획득할 수 있도록 함으로써, 공공 네트워크를 통해 암호화된 암호데이터($\{M\}K_s$)를 유통하더라도 데이터에 대한 향상된 보안성을 제공할 수 있다.

<62> 이상에서는 본 발명에서 특정의 바람직한 실시 예에 대하여 도시하고 또한 설명하였다. 그러나, 본 발명은 상술한 실시 예에 한정되지 아니하며, 특허 청구의 범위에서 첨부하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능할 것이다.

【특허청구범위】**【청구항 1】**

할당된 고유아이디정보인 고유비밀키(Kh)를 저장하는 고유비밀키 저장부;

공공 네트워크를 통해 수신된 상기 고유비밀키(Kh)에 의해 암호키(Ks)가 암호화된 모듈비밀키($\{Ks\}Kh$)로부터 상기 암호키(Ks)를 디코딩하는 제1디코딩부; 및

상기 암호키(Ks)를 이용하여 상기 공공 네트워크를 통해 수신된 데이터(M)가 암호화된 암호데이터($\{M\}Ks$)로부터 상기 데이터(M)를 디코딩하는 제2디코딩부를 포함하는 것을 특징으로 하는 보안 판독 장치.

【청구항 2】

제 1항에 있어서,

공공 네트워크를 통해 전송된 상기 모듈비밀키($\{Ks\}Kh$)를 저장하고, 상기 제1디코딩부의 제어에 따라 저장된 상기 모듈비밀키($\{Ks\}Kh$)를 상기 제1디코딩부로 출력하는 모듈비밀키 저장부; 및

상기 제1디코딩부에서 디코딩된 상기 암호키(Ks)를 저장하고, 상기 제2디코딩부의 제어에 따라 저장된 상기 암호키(Ks)를 상기 제2디코딩부로 출력하는 암호키 저장부를 더 포함하는 것을 특징으로 하는 보안 판독 장치.

【청구항 3】

통신단말기에서 요구한 데이터를 서비스하는 데이터 서비스 공급장치에 있어서,

상기 통신단말기에 제공하기 위한 상기 데이터(M)를 저장하는 데이터 데이터베이스;

상기 통신단말기에 마련되어 상기 데이터를 판독하는 보안판독모듈의 고유아이디정보에 대응하는 고유비밀키(Kh)를 저장하는 고유비밀키 데이터베이스;

상기 통신단말기와 공공네트웍을 통해 상호 통신을 수행하는 송수신부;

상기 데이터(M)를 해당 암호키(Ks)를 이용하여 암호화하는 데이터 암호화부;

상기 암호키(Ks)를 상기 고유비밀키(Kh)를 이용하여 암호화하는 고유비밀키 암호화부; 및

상기 데이터 암호화부 및 상기 고유비밀키 암호화부의 암호화 동작을 제어하고, 암호화된 암호데이터($\{M\}Ks$) 및 모듈비밀키($\{Ks\}Kh$)를 상기 공공네트웍을 통해 상기 통신단말기에 제공하도록 상기 송수신부를 제어하는 제어부를 포함하는 것을 특징으로 하는 데이터 서비스 공급장치.

【청구항 4】

제 3항에 있어서,

상기 보안판독모듈은,

상기 보안판독모듈에 할당된 상기 고유아이디정보인 상기 고유비밀키(Kh)를 저장하는 고유비밀키 저장부;

상기 고유비밀키(Kh)를 이용하여, 상기 송수신부에서 제공된 상기 모듈비밀키($\{Ks\}Kh$)로부터 상기 암호키(Ks)를 디코딩하는 제1디코딩부; 및

상기 암호키(K_s)를 이용하여, 상기 송수신부에서 제공된 상기 암호데이터($\{M\}K_s$)로부터 상기 데이터(M)를 디코딩하는 제2디코딩부를 포함하는 것을 특징으로 하는 데이터 서비스 공급장치.

【청구항 5】

제 4항에 있어서,

상기 보안판독모듈은,

상기 송수신부에서 제공된 상기 모듈비밀키($\{K_s\}K_h$)를 저장하고, 상기 제1디코딩부의 제어에 따라 저장된 상기 모듈비밀키($\{K_s\}K_h$)를 상기 제1디코딩부로 출력하는 모듈비밀키 저장부; 및

상기 제1디코딩부에서 디코딩된 상기 암호키(K_s)를 저장하고, 상기 제2디코딩부의 제어에 따라 저장된 상기 암호키(K_s)를 상기 제2디코딩부로 출력하는 암호키 저장부를 더 포함하는 것을 특징으로 하는 데이터 서비스 공급장치.

【청구항 6】

a) 할당된 고유아이디정보인 고유비밀키(K_h)에 대해 암호화된 모듈비밀키($\{K_s\}K_h$)의 수신여부를 판단하는 단계;

b) 상기 모듈비밀키($\{K_s\}K_h$)가 수신된 것으로 판단되면, 상기 고유비밀키(K_h)를 이용하여 상기 모듈비밀키($\{K_s\}K_h$)로부터 암호키(K_s)를 디코딩하는 단계;

c) 전송을 요구한 데이터(M)가 암호키(Ks)에 의해 암호화된 암호데이터({M}Ks)의 수신 여부를 판단하는 단계; 및

d) 상기 암호데이터({M}Ks)가 수신된 것으로 판단되면, 상기 암호키(Ks)를 이용하여 상기 암호데이터({M}Ks)로부터 상기 데이터(M)를 디코딩하는 단계를 포함하는 것을 특징으로 하는 보안 판독 장치를 이용한 암호 판독 방법.

【청구항 7】

통신단말기에서 요구한 데이터를 서비스하는 데이터 서비스 공급장치를 이용한 데이터 서비스 공급방법에 있어서,

상기 통신단말기로부터 공공 네트워크를 통해 전송된 데이터(M)의 전송 요구를 수신하는 단계;

수신된 상기 데이터의 전송 요구에 따라 상기 데이터(M)를 해당 암호키(Ks)를 이용하여 암호화하는 단계;

수신된 상기 데이터의 전송 요구에 따라 상기 통신단말기에 마련되어 상기 데이터(M)가 암호화된 암호데이터({M}Ks)를 디코딩하는 보안판독모듈의 고유아이디정보에 대응하는 고유비밀키(Kh)를 이용하여 상기 암호키(Ks)를 암호화하는 단계; 및

암호화된 암호데이터({M}Ks) 및 모듈비밀키({Ks}Kh)를 상기 공공네트워크를 통해 상기 통신단말기에 전송하는 단계를 포함하는 것을 특징으로 하는 데이터 서비스 공급장치를 이용한 데이터 서비스 공급방법.

【청구항 8】

제 7항에 있어서,

상기 통신단말기에 마련된 상기 보안판독모듈은,

상기 보안판독모듈에 할당된 상기 고유아이디정보인 상기 고유비밀키(Kh)를 저장하는 고유비밀키 저장부;

상기 고유비밀키 암호화부에서 암호화된 상기 모듈비밀키($\{K_s\}K_h$)로부터 상기 암호키(K_s)를 디코딩하는 제1디코딩부; 및

상기 암호키(K_s)를 이용하여 상기 데이터 암호화부에서 암호화된 상기 암호데이터($\{M\}K_s$)로부터 상기 데이터(M)를 디코딩하는 제2디코딩부를 포함하는 것을 특징으로 하는 데이터 서비스 공급장치를 이용한 데이터 서비스 공급방법.

【청구항 9】

제 8항에 있어서,

상기 보안판독모듈은,

상기 송수신부로부터 제공된 상기 모듈비밀키($\{K_s\}K_h$)를 저장하고, 상기 제1디코딩부의 제어에 따라 저장된 상기 모듈비밀키($\{K_s\}K_h$)를 상기 제1디코딩부로 출력하는 모듈비밀키 저장부; 및

상기 제1디코딩부에서 디코딩된 상기 암호키(K_s)를 저장하고, 상기 제2디코딩부의 제어에 따라 저장된 상기 암호키(K_s)를 상기 제2디코딩부로 출력하는 암호키 저장부를

더 포함하는 것을 특징으로 하는 데이터 서비스 공급장치를 이용한 데이터 서비스 공급 방법.

【청구항 10】

공공 네트워크를 통해 데이터(M)가 암호키(Ks)에 의해 암호화된 암호데이터($\{M\}Ks$)를 수신하는 이동통신 단말기에 있어서,

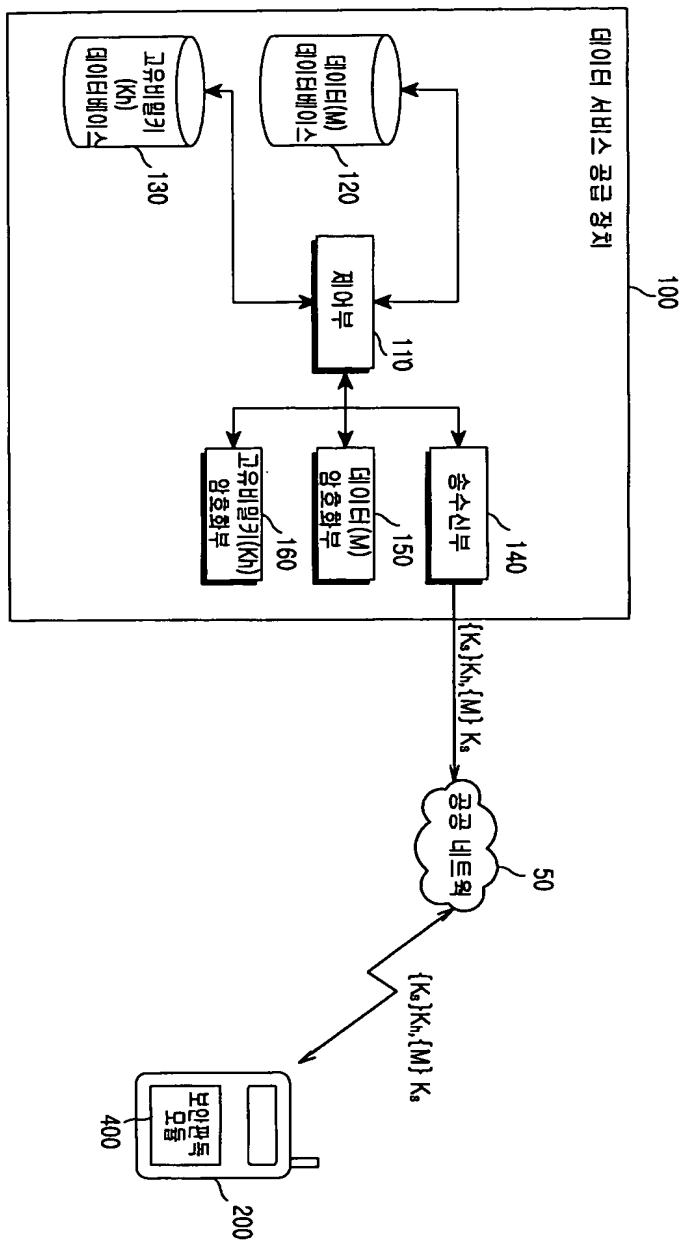
할당된 소정의 고유 아이디 정보인 고유비밀키(Kh)를 저장하는 고유비밀키 저장부 ;

상기 고유비밀키(Kh)로 암호화된 모듈비밀키($\{Ks\}Kh$)를 수신하면 상기 모듈비밀키($\{Ks\}Kh$)로부터 암호키(Ks)를 디코딩하는 제1디코딩부; 및

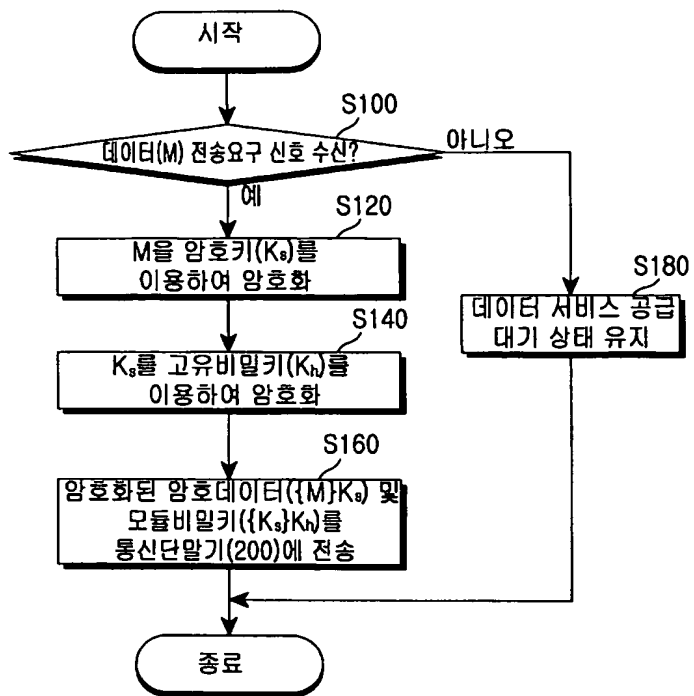
상기 암호키(Ks)를 이용하여 상기 암호데이터($\{M\}Ks$)로부터 상기 데이터(M)를 디코딩하는 제2디코딩부를 포함하는 것을 특징으로 하는 보안 판독 장치.

【도면】

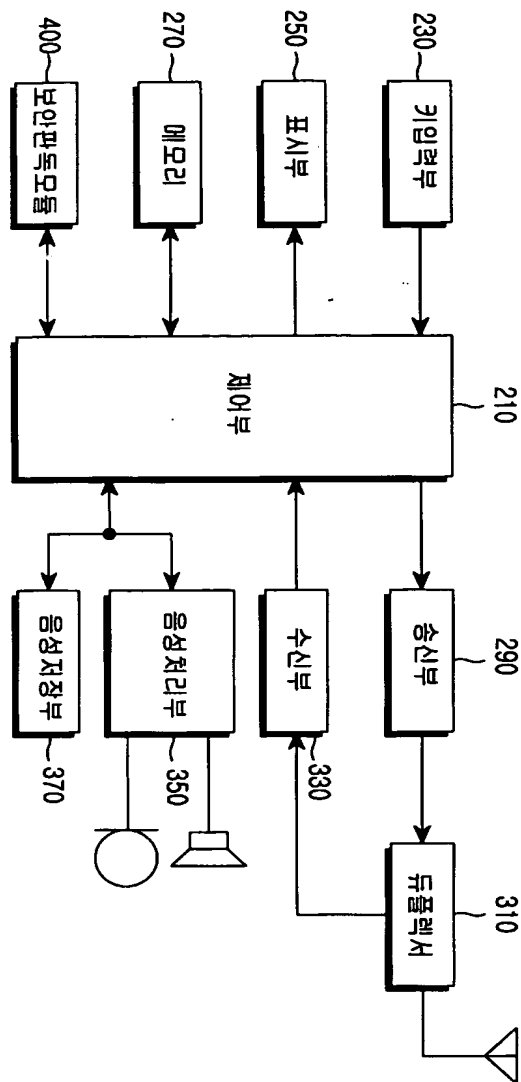
【도 1】



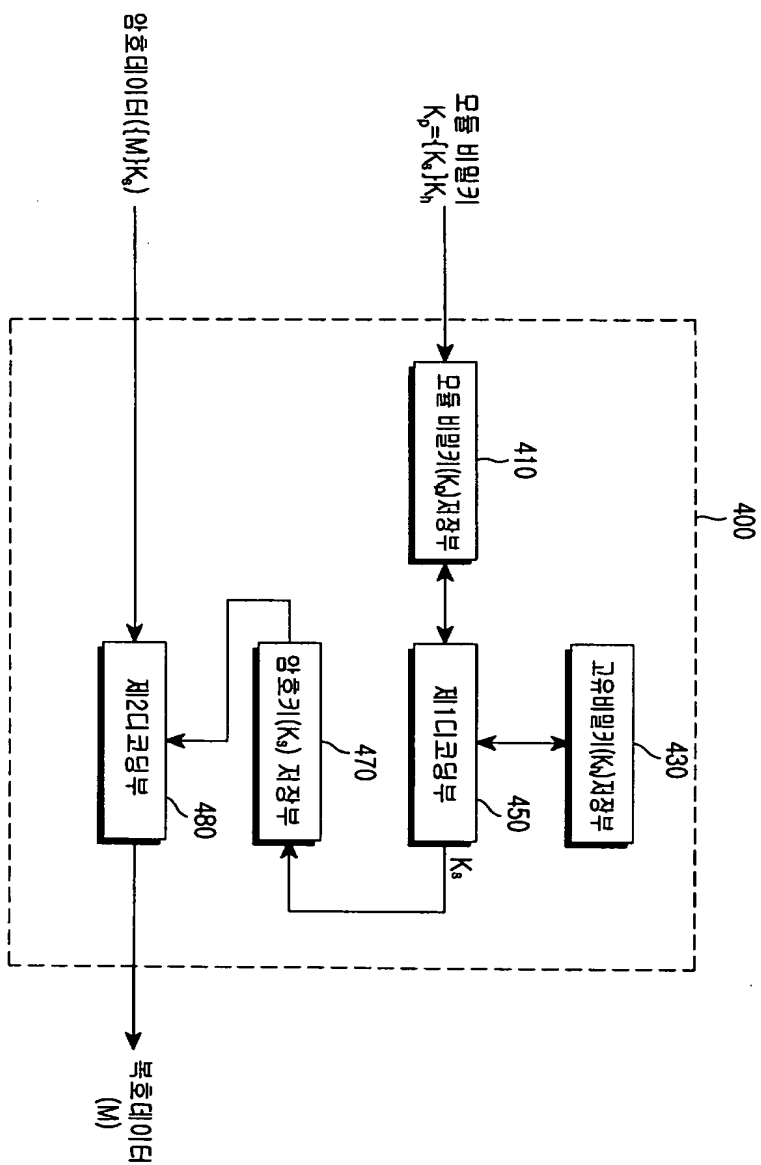
【도 2】



【도 3】



【도 4】



【도 5】

